UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

EUDI ed EBSI: Architettura, Sicurezza e Sfide di Conformità al GDPR

Relatore: Prof. Migliardi Mauro

Laureando: Toccane Alessandro

ANNO ACCADEMICO 2024 – 2025

Data di laurea 25 settembre 2025

CAPITOLO 1: Introduzione a EUDI

Contesto e intenzioni:

L'identità digitale europea è un sistema che consente a privati cittadini, a imprese o a pubbliche amministrazioni di identificarsi online, il tutto in maniera sicura secondo un regolamento chiamato eIDAS 2.0.

Lo scopo ultimo dell'identità digitale europea è quello di poter permettere al soggetto che si identifica di condividere solo le informazioni personali che sceglie di condividere, avendo una piattaforma che garantisca per lui, eliminando anche la dipendenza dai sistemi privati (es. login tramite Google o Facebook).
Il servizio sarà attivo in tutti i paesi dell'Europa, facilitando l'accesso a molti dei servizi pubblici e privati come firme elettroniche o accesso a servizi sanitari.

La riservatezza dei dati personali dei cittadini europei è la priorità di questo progetto.
I rischi per gli utenti legati alla diffusione di dati personali riguardano per esempio la creazione di profili falsi, la profilazione e il tracciamento sia sul web che al di fuori.
ElonJet l'account X (all'epoca Twitter) creato da Jack Sweeney pensato per tracciare e condividere in tempo reale gli spostamenti del jet privato di Elon Musk è un ottimo esempio di come il tracciamento e la diffusione di dati pubblici in rete possa costituire una minaccia alla privacy dei cittadini.
Musk ha offerto allo studente dell'università della Florida all'epoca diciannovenne cinquemila dollari, per chiudere l'account.
È necessaria dunque una tutela riguardo la diffusione di dati.

Un'identità digitale è necessaria anche e soprattutto al cittadino che non è una figura pubblica per identificarsi online e accedere a servizi pubblici e privati senza dover usare documenti fisici.
L'accesso ai servizi online (come INPS, agenzia delle entrate, banche, università…) sarà semplificato attraverso un'unica modalità di accesso, cioè non servirà più ricordare la password associata al servizio corrispondente.
Sarà possibile conservare documenti fisici come carta di identità, patente ecc. in un formato digitale riconosciuto e firmare elettronicamente e con valore legale contratti o documenti ufficiali in tutta Europa.

Molti paesi adottano già sistemi di identità digitale:

- Italia, con SPID usato per accedere ai servizi della pubblica amministrazione
- Germania, Svezia, Belgio, Danimarca, Estonia, Finlandia, Repubblica Ceca, Francia, Romania e Liechtenstein con eID per l'autenticazione online
- Belgio si usa anche itsme, un applicativo che permette l'autenticazione se si usa uno smartphone
- Spagna con DNle un documento di identità elettronico usato anche per autenticarsi a servizi web e firma digitale

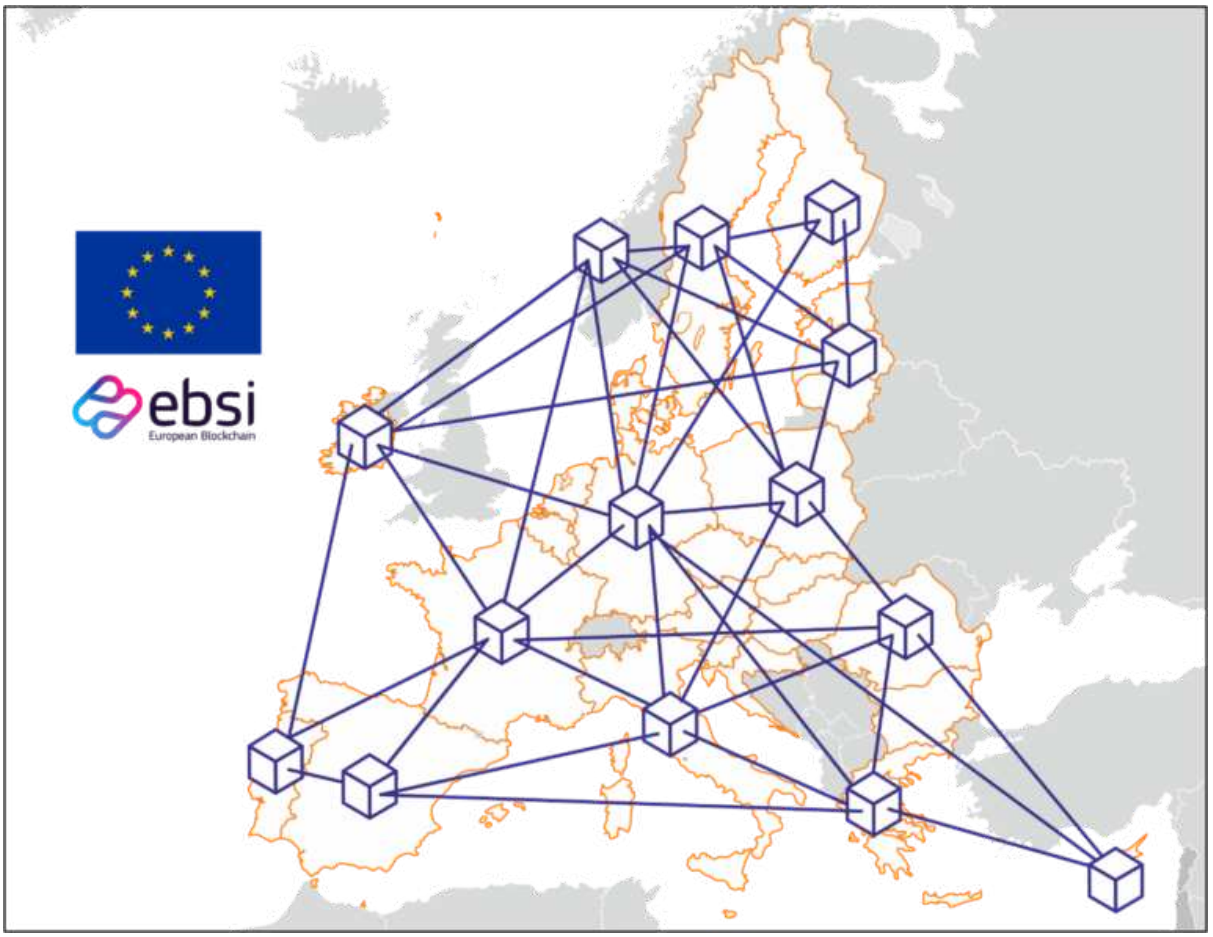
A partire dal 2026 EUDI andrà progressivamente a sostituire i servizi sopraelencati. Nessuna delle piattaforme inoltre garantisce la piena interoperabilità tra tutti gli Stati dell'Ue come previsto da eIDAS 2.0.

EIDAS 2.0 è la seconda versione del regolamento eIDAS (Electronic Identification, Authentication and Trust Services) l'insieme di norme approvate dall'Unione Europea per migliorare l'identificazione digitale e servizi associati in Europa.
La versione originale di eIDAS, nata nel 2014 ha stabilito delle regole comuni in tutta l'Unione per il riconoscimento di firma elettronica, servizi di certificazione e sigilli digitali.
La necessità di un nuovo regolamento nasce dal principio che l'eIDAS originale, lasciava ai singoli Stati la decisione sul creare o meno un sistema di identità digitale interoperabile e solo pochi stati si sono mossi in questo senso.
Viene dunque proposto nel 2021, con approvazione nel 2023, eIDAS 2.0 che obbliga tutti gli Stati membri a offrire un'identità digitale valida e comune in tutta europa.

CAPITOLO 2: Architettura EUDI, EBSI e introduzione a blockchain

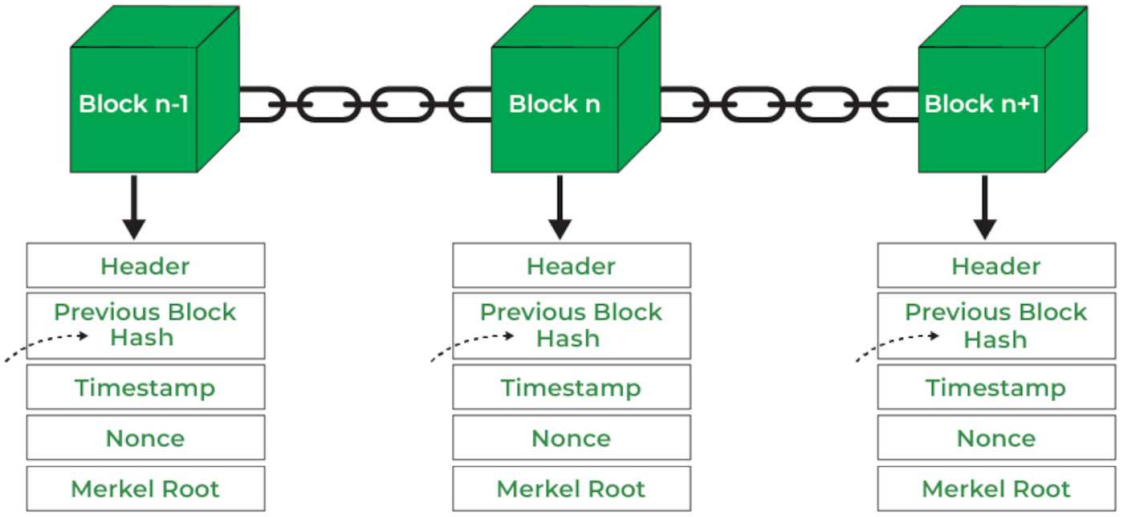
EBSI:

In questo contesto nasce anche EBSI (European Blockchain Services Infrastructure) un'iniziativa della commissione europea e dell'European Blockchain Partnership (EBP) nata per utilizzare la Blockchain nei servizi pubblici dell'UE, il suo obiettivo è quello di fornire un'infrastruttura sicura e decentralizzata per lo scambio di dati.
EBSI è dunque una rete blockchain europea progettata per fornire servizi pubblici digitali in cui gli Stati membri e le istituzioni gestiscono i nodi della blockchain per verificare e scambiare informazioni in modo sicuro.
EBSI è dunque l'infrastruttura tecnologica utilizzata dal wallet.



Blockchain:
Blockchain è una tecnologia che consente di registrare dati in modo sicuro, trasparente e immutabile.
È un registro digitale distribuito che non risiede in un solo computer ma è condiviso tra molti nodi a formare una rete.
I dati (che possono essere transazioni, informazioni, contratti, ecc.) vengono raggruppati in strutture dette blocchi.
Ogni blocco è formato da:

- un insieme di dati
- Un hash, cioè un codice identificativo
- L'hash del blocco precedente



I blocchi sono collegati fra loro secondo un ordine cronologico formando una catena, da qui blockchain.
L'utilizzo di una blockchain consente di avere:

- decentralizzazione, non esiste un'autorità centrale, l'autorità viene distribuita su più nodi della rete
- Trasparenza, perché ogni nodo della rete è in grado di visualizzare i dati registrati
- Sicurezza, infatti grazie alla decentralizzazione in combinazione a crittografia, l'alterazione dei dati risulta molto complessa
- Immutabilità, una volta scritto, il dato non può essere cancellato o modificato

La tecnologia blockchain può essere di diversi tipi, in base alla finalità di utilizzo, esistono in particolare

- blockchain pubbliche, cioè aperte a tutti (eg. Ethereum)

- Blockchain private, cioè gestite da organizzazioni private (eg. Hyperledger Fabric)
- Blockchain Consortium, gestite da agenzie o aziende tra loro fidate

Dato che i nodi devono mettersi d'accordo su cosa aggiungere alla catena e sull'ordine in cui farlo si rende necessario l'utilizzo dei Meccanismi di Consenso.
Ne vengono definiti principalmente quattro:

- Proof of Work (PoW): i nodi (miner) risolvono un problema matematico, il primo che ci riesce, aggiunge il blocco alla blockchain e si intasca una commissione (usato ad esempio in bitcoin)
- Proof of Stake (PoS): i partecipanti (validatori) vengono scelti in basi a quanti token mettono in "staking" cioè utilizzano come garanzia, questo meccanismo seppur utilizza meno energia del mining, può favorire i ricchi perché chi possiede più token possiede idealmente più potere (usato da Ethereum)
- Delegated Proof of Stake (DPoS): gli utenti votano dei delegati che scrivono a nome di tutti
- Proof of Authority (PoA): solo nodi autorizzati possono scrivere sulla blockchain

comprendere caratteristiche e tipologie di blockchain è essenziale per analizzare come EBSI e di conseguenza EUDI, riusciranno a garantire privacy e sicurezza dei dati e interoperabilità.

Differenze tra cripto blockchain e EBSI:
Le cose che accomunano cripto valute e EBSI sono:

- La catena di blocchi contenente transazioni o dati verificabile, un registro distribuito il distributed Ledger Technology (DLT)
- L'idea di decentralizzazione
- L' immutabilità dei dati

Le Blockchain legate alle criptovalute sono definite pubbliche e permissionless cioè chiunque può partecipare come nodo della rete, di fatto non esiste nessuna autorità di controllo poiché la Blockchain è altamente decentralizzata.
EBSI al contrario è definita permissioned e consortile, solo enti autorizzati possono gestire i nodi, c'è quindi una minore decentralizzazione rispetto alle blockchain pubbliche.

Il consenso è il cuore di una Blockchain, garantisce che tutti i partecipanti abbiano la stessa versione del registro e che le transazioni siano affidabili.
È quindi la tecnica attraverso la quale i nodi concordano sulla validità delle transazioni, garantendo così la sicurezza della rete.

EBSI non ha bisogno di meccanismi di consenso come PoW visto che i nodi della rete sono affidabili, si usa invece BFT, Byzantine Fault Tolerance.
BFT garantisce che il sistema possa comunque funzionare seppure qualche nodo della rete risulta compromesso.
Anche se le transazioni sono pubbliche nelle criptovalute gli utenti sono anonimi o coperti da pseudonimi così facendo ne garantiscono la privacy.
Su EBSI si usano verified credentials (VC) e decentralized identifiers (DID), l'utente è in grado di decidere chi accede ai dati ed essendo GDPR compliant verrà garantito il diritto all'oblio.

Verified credentials e Decentralized Identifiers:
I decentralized identifiers (DID) sono identificatori digitali univoci e permanenti, creati secondo lo standard W3C che non dipendono da un registro centrale.
Ha una forma del tipo
did:ebsi:idUnivoco

dove:
- did, indica che si tratta di un Decentralized Identifier
- ebsi, indica il metodo, cioè come e dove trovare le informazioni su quel identificatore, in sostanza è il tipo di protocollo
- idUnivoco, come suggerisce il nome, l'effettivo identificatore

Ogni DID è associato a un DID document cioè un file che contiene
- Chiavi pubbliche, servono per verificare le firme digitali
- Endpoint di servizio
- Metadati, versione, data di creazione ecc.

Il DID e il relativo DID document di una persona fisica, vengono generati e custoditi all'interno del suo wallet digitale che crea una coppia di chiavi crittografiche (una privata e una pubblica).
La chiave pubblica dell'utente viene inserita nel DID document che però in conformità al regolamento eIDAS, non viene pubblicato direttamente sulla blockchain (così non vengono esposti dati personali).
Sulla catena vengono invece registrati identificatori utilizzati per validare i DID degli utenti senza rivelarne direttamente l'identità.
Quando viene rilasciata una Verifiable Credential (VC), l'emittente la firma con la sua chiave privata.
Il destinatario della VC può verificare la validità della firma recuperando le informazioni di verifica dal DID document su cui fa un controllo utilizzando la chiave pubblica.

Le Verifiable Credentials sono attestazioni digitali che dichiarano delle informazioni associate a un soggetto e sono firmate digitalmente dall'ente che le emette.
Una VC è un documento che contiene

- Issuer, cioè l'entità che la emette
- Subject, il soggetto a cui è riferita
- Claim, le informazioni da attestare
- Proof, la firma digitale dell'Issuer

La verifiable credential permette di condividere informazioni certificate senza dover rivelare tutto secondo il principio di selective disclosure.
Ad esempio, uno studente che si candida per un lavoro potrebbe mostrare attraverso il wallet solo il fatto che ha conseguito una laurea nel settore richiesto dall'azienda senza dover comunicare il voto o la data in cui si è laureato.
Definiamo in questo contesto tre figure, già parzialmente discusse :

- Issuer, l'entità che crea e rilascia una credenziale digitale firmata
- Holder, è il titolare della credenziale che l'issuer rilascia
- Verifier, l'entità che richiede e verifica delle informazioni fornite dall'issuer (eg. un titolare di lavoro che verifica che un candidato abbia un diploma richiesto in sede di application)

Come operano quindi in collaborazione DID e VC nel sistema EBSI?
Il DID identifica in maniera univoca gli utenti o le entità (sia Issuer che Holder ma anche il Verifier).
La Verifiable Credential è il contenuto certificato che un Issuer associa al DID del suo titolare, questo attestato viene detenuto dall'utente in modo tale da non dover contattare l'issuer ogni volta.
La detenzione degli attestati garantisce controllo diretto sui dati oltre che privacy, l'issuer non deve poter sapere quando e dove vengono presentate le credenziali.
La verifica si basa sulla firma dell'issuer e sulle informazioni pubbliche del DID document.

Struttura blocco EBSI:
Ogni blocco avrà una struttura simile a quella delle blockchain pubbliche, verrà cioè divisa in un Header, contenente i metadati e un Body che contiene le transazioni.
L'intestazione del blocco (Header) conterrà tra i suoi parametri:

- block hash, cioè l'identificativo del blocco
- Hash del blocco precedente
- Timestamp, cioè data e ora della creazione del blocco
- Firma del nodo validatore, cioè il via libera dall'ente autorizzato

il body avrà invece un aspetto di questo tipo

```
{
  "transaction_id": "12345abc",
  "issuer": "Università di Padova",
  "recipient": {
    "DID": "did:ebsi:123xyz",
    "name": "Alessandro Toccane"
  },
  "credential": {
    "type": "Diploma",
    "degree": "Laurea triennale in Ingegneria Informatica",
    "issued_date": "2025-09-22"
  },
  "signature": "sig_456def"
}
```

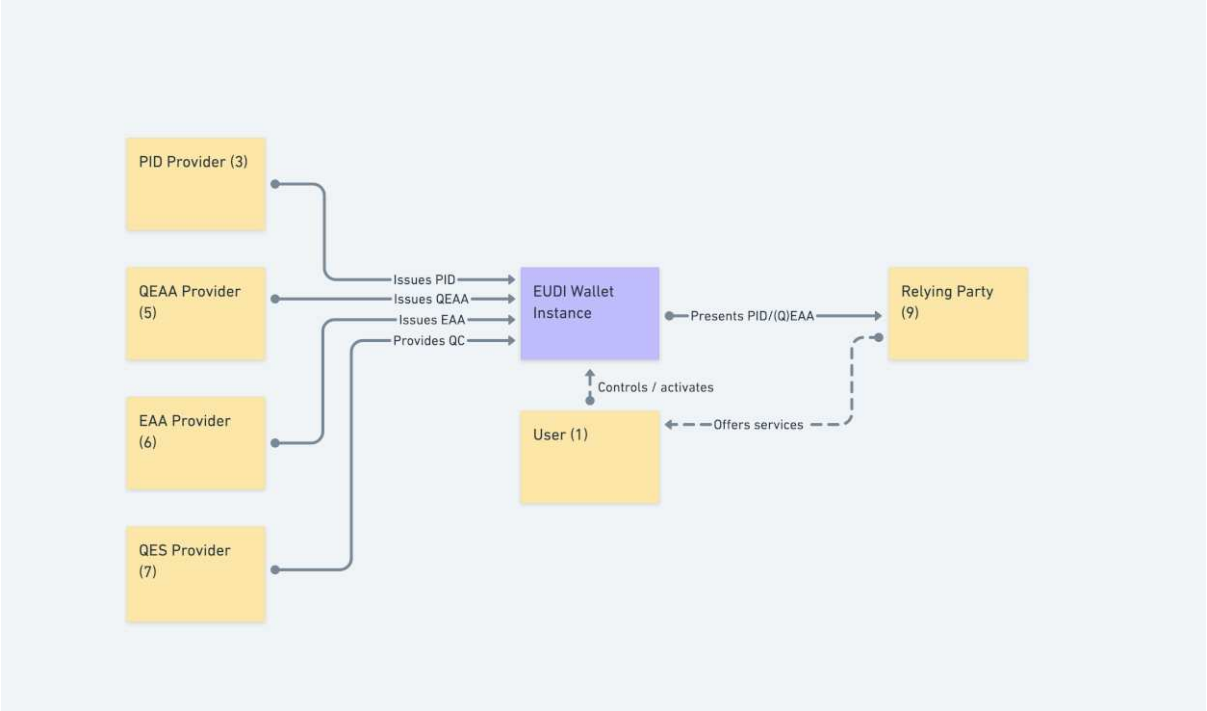

Il nodo validatore, che nel caso sopra potrebbe essere il ministero dell'istruzione, verifica la transazione e firma il blocco che una volta approvato viene aggiunto alla blockchain.
Ovviamente quello sopra è solo un esempio di come un blocco della catena potrebbe apparire, nella realtà, EBSI memorizza sul ledger (il registro dove vengono inserite tutte le transazioni) solo impronte crittografiche (hash) e metadati, non i dati personali in chiaro, per conformità al GDPR.

ARF:

Dopo aver parlato del ruolo di EBSI come infrastruttura europea per i servizi digitali basati su blockchain, è utile soffermarsi anche su ARF, Architecture Reference Framework.
Si tratta del modello architetturale di riferimento proposto dalla commissione europea, un modello architetturale a più alto livello rispetto al "substrato" blockchain EBSI.
ARF definisce un ecosistema più ampio in cui vengono ben definiti i blocchi principali

Attestazioni elettroniche e certificati qualificati:
Uno dei blocchi principali descritti da ARF sono le attestazioni elettroniche e i certificati qualificati che garantiscono affidabilità e riconoscimento giuridico delle identità digitali e delle transazioni.
In primo luogo si può parlare del PID (Person Identification Data) che rappresenta l'insieme minimo di attributi identificativi (es. nome, cognome, data di nascita, ecc.) , validati da un'autorità competente e necessari per attestare l'identità legale di una persona.
Oltre all'insieme di attributi utilizzati per definire una persona, esistono attributi aggiuntivi (come titoli di studio, abilitazioni professionali, certificati medici, ecc.) che

vengono rilasciati da fornitori qualificati e dotati di validità anche legale, i QEAA (Qualified Electronic Attestation of Attributes).
Oltre a questi però possono esistere altri attestati che hanno valore legale nei contesti specifici ma non vengono rilasciati da enti accreditati (come titoli di viaggio, abbonamenti a trasporti pubblici, certificati di appartenenza a ordini professionali locali, ecc.) gli EAA (Electronic Attestation of Attributes).
Ci sono infine i QES (Qualified Electronic Signature) che rappresenta lo strumento con cui l'utente può sottoscrivere digitalmente documenti in maniera riconosciuta in tutta l'unione europea.
Quindi PID, QEAA, EAA possono essere implementati come Verified Credentials (VC) e quindi rappresentati, condivisi e validati tramite essi, mentre QES è un meccanismo crittografico basato su un certificato qualificato rilasciato da un QES provider.



Architettura EUDI:

L'architettura dell'EUDI wallet è costruita secondo i principi di centralità dell'utente, interoperabilità, privacy e security by design, traducendo i requisiti già citati del regolamento eIDAS 2.0 in un'infrastruttura tecnica affidabile conforme agli standard europei.
Al centro dell'ecosistema vi è il dispositivo dell'utente che ospita l'istanza del portafoglio (wallet instance) tipicamente un'applicazione mobile per le persone fisiche o un server per le persone giuridiche.

La sicurezza crittografica dell'istanza del portafoglio è garantita dal Wallet Secure Cryptographic Device (WSCD) e dalla Wallet Secure Cryptographic Application (WSCA), componenti che gestiscono chiavi e firme digitali in ambienti sicuri, sia integrati nei dispositivi (come Secure Enclave per iPhone e StrongBox per Android) sia remoti.
WSCD è l'hardware che custodisce le chiavi mentre WSCA è il software che le utilizza.

Il wallet interagisce con le Relying Party (l'ente che richiede le informazioni) attraverso diverse modalità (se utente e relying party sono fisicamente vicini si possono usare tecnologie come NFC o Bluetooth, altrimenti per sessioni in remoto il device gestisce in sé o monitora la sessione), con le garanzie di sicurezza di protocolli come OpenID4VP e ISO/IEC18013-5.
Fondamentale è anche il ruolo dei fornitori del portafoglio, responsabili di assicurare la conformità tecnica e normativa del wallet, attraverso processi di certificazione previsti dalle linee guida europee.
L'architettura nel suo complesso mira a garantire un sistema scalabile, sicuro e interoperabile in grado di supportare servizi transfrontalieri e rafforzare la fiducia degli utenti nella gestione della propria identità digitale.

OpenID4VP e ISO/IEC18013-5:
OpenID4VP (OpenID for Verifiable Presentation) è un protocollo di autenticazione che consente a un utente di presentare in modo sicuro le proprie verifiable credential in scenari remoti a un relying party.
Lo standard ISO/IEC 18013-5 è lo standard pensato per la trasmissione sicura di credenziali digitali in contesti di prossimità come NFC o Bluetooth.

CAPITOLO 3: criticità tecniche, sicurezza

Attacchi alla blockchain:

Sebbene la tecnologia blockchain offra per sua natura caratteristiche di resistenza alla manomissione, essa non è immune a possibili minacce.
Dividiamo i possibili attacchi in due macro categorie

- attacchi al consenso che comprendono ad esempio il 51% attack, in cui un gruppo di nodi validatori ottiene il controllo della maggioranza del potere di validazione, potendo così manipolare o riscrivere transazioni. Dato che ci si trova in un contesto di blockchain permissioned il rischio di questo scenario è ridotto ma rimane comunque un attacco possibile.
- attacchi alla rete come il Sybil attack (creazione di nodi falsi), l'Eclipse attack (controllo delle informazioni su un nodo) o i DDOS (saturare le risorse di un nodo)

Attacchi alla persona:

Un attacco informatico che colpisce direttamente una persona non è solo un evento tecnico, ma può trasformarsi in un'esperienza devastante nella vita quotidiana di un individuo.
Essere vittima di un furto d'identità significa, ad esempio ritrovarsi improvvisamente esclusi da servizi essenziali, scoprire che qualcuno ha stipulato contratti a proprio nome o anche essere monitorati.
La perdita di controllo sulla propria identità digitale può generare ansia e senso di vulnerabilità oltre che sfiducia nel sistema EUDI oltre che nelle istituzioni.
Le principali minacce includono il phishing e tecniche di social engineering, che mirano a ingannare l'utente inducendolo a condividere credenziali o ad autorizzare accessi indesiderati.
Esistono poi gli attacchi mirati a intercettare e riutilizzare credenziali come i man in the middle.
A questi si aggiungono poi i rischi di tracciamento che possono portare a profilazioni non autorizzate.
Anche in presenza di un'infrastruttura blockchain sicura l'anello più debole resta spesso l'utente, è quindi necessario adottare misure tecniche ma anche di consapevolezza per proteggere l'identità digitale.

Attacchi da governi o aziende:

Un ulteriore categoria di minacce non riguarda né la singola infrastruttura tecnologica né l'utente individuale ma nasce dall'uso improprio o dall'abuso da parte di attori istituzionali o aziendali.
Governi o imprese che controllano nodi della rete o operano come issuer o verifier potrebbero, ad esempio, sfruttare la loro posizione privilegiata per raccogliere dati in modo massivo, effettuare attività di sorveglianza indebita o imporre pratiche discriminatorie nell'accesso ai servizi.
L' immutabilità del registro, se usata senza limiti, rischia di trasformarsi in uno strumento di controllo più che di garanzia.
Un esempio concreto di queste preoccupazioni può essere trovato nel caso Paragon, legato al presunto uso improprio da parte del governo italiano di un software di sorveglianza israeliano che si suppone sia stato utilizzato per lo spionaggio ai danni di due attivisti e giornalisti.
Qualche anno prima tra il 2010 e il 2020 un altro spyware, Pegasus è stato utilizzato da diversi governi europei per il monitoraggio mirato di oppositori politici oltre che attivisti e giornalisti.
I casi hanno alimentato un ampio dibattito pubblico sulla possibilità che strumenti digitali, nati per garantire sicurezza o efficenza, possano invece essere impiegati per attività di spionaggio e controllo dei cittadini.
Analogamente, aziende private potrebbero utilizzare le credenziali digitali non solo per verificare l'identità degli utenti ma anche per tracciarne i comportamenti, costruendo profili commerciali dettagliati o scambiando dati con terze parti senza consenso informato.
Questi scenari rappresentano forme di attacco più subdole perché non si manifestano in maniera evidente, la vera minaccia non è più tecnica ma sociale e politica.

Dipendenza da infrastrutture extraeuropee:

La questione dell'indipendenza dell'infrastruttura europea EUDI/EBSI da piattaforme extraeuropee intreccia aspetti di sovranità digitale, sicurezza e tutela dei dati.
Oggi una quota significativa dei dati e servizi digitali europei risiede su server di aziende straniere, soprattutto statunitensi, il che solleva seri interrogativi sull'autonomia tecnologica del continente.
Questa dipendenza offre indubbi vantaggi in termini di efficienza ma espone l'Europa a vulnerabilità geopolitiche: un interruzione improvvisa dei servizi cloud esteri, ad esempio per politiche nazionali o conflitti, potrebbe paralizzare interi settori pubblici o privati, con danni enormi per società ed economia.

Inoltre, affidarsi a fornitori non europei significa sottostare a normative di altri paesi: ad esempio, la legge statunitense Cloud Act permette alle autorità USA di requisire dati dalle aziende tech americane anche se ospitati in data center europei, creando un conflitto con le rigorose tutele UE sulla privacy e sfociando in contenziosi diplomatici, come dimostra la vicenda dell'accordo Privacy Shield, invalidato dalla corte di giustizia UE nel 2020 poiché la corte ha stabilito un insufficiente livello di protezione dei dati personali.
Viene dunque introdotto nel 2023 il nuovo EU-US Data Privacy Framework (DPF) con l'obiettivo di garantire maggiore sicurezza nel trasferimento dei dati personali.
Sullo scenario globale, gli attori principali sono gli Stati Uniti e la Cina, le cui big tech dominano il mercato del cloud e dei servizi digitali, basti pensare a colossi come Amazon, Google, Microsoft e Alibaba.
Questa dominanza industriale porta con sé potenziali frizioni con gli interessi europei, poiché né l'ordinamento statunitense né quello cinese assicurano garanzie equivalenti a quelle europee in tema di protezione dei dati, privacy e controllo delle informazioni.
Proprio per questo l'UE ha fatto della sovranità digitale una priorità strategica, mirando a ridurre la dipendenza da tecnologie e infrastrutture extra UE tramite lo sviluppo di soluzioni proprie.
Dotarsi di una identità digitale autonoma e sovrana significa infatti per l'Europa ridurre l'affidamento a fornitori esterni e offrire ai cittadini un mezzo di identificazione gestito interamente nel perimetro normativo europeo, in linea con i valori europei di privacy e sicurezza.
Ciò consente di tutelare i dati personali mantenendoli sotto giurisdizione europea e di proteggere meglio le infrastrutture critiche.
Allo stesso tempo, l'UE sta investendo per rafforzare la propria autonomia tecnologica nel cloud: emblematico è il progetto Gaia X, iniziativa lanciata da Francia, e Germania nel 2019 che mira a creare un ecosistema cloud federato, basato su standard europei di trasparenza interoperabilità e sicurezza, offrendo così alle imprese, un'alternativa ai provider USA e garantendo che i dati siano gestiti secondo le norme del continente indipendentemente dal fornitore.
Tuttavia Gaia X ha dei grossi limiti legati alla partecipazione aperta, grandi attori statunitensi hanno aderito al progetto assumendo anche dei ruoli significativi nei gruppi di lavoro e di decisioni strategiche.
Questo è finito per generare dubbi e perplessità, se aziende USA cioè quelle da cui l'Europa vuole ridurre la dipendenza partecipano alla definizione delle regole e dell'ecosistema Gaia X allora il rischio è che il progetto finisca per avere proprio la dipendenza che intendeva eliminare.

CAPITOLO 4: contromisure punto per punto

Contromisure per attacchi alla blockchain:

La riduzione dei rischi legati agli attacchi alla blockchain richiede un approccio multilivello.
In primo luogo, l'adozione di un modello permissioned con rigorose procedure di onboarding dei nodi e autenticazione forte dei validatori riduce significativamente l'esposizione ad attacchi al consenso e tentativi di infiltrazione di nodi malevoli.
In pratica solo organizzazioni approvate nell'ambito dell'European Blockchain Partnership (EBP) possono entrare a far parte della rete, previo un processo di onboarding formale che prevede la verifica del rispetto dei requisiti tecnici minimi.
Per autenticazione forte si intende che il modello di consenso è QBFT (Quorum-based Byzantine Fault Tolerance) cioè che richiede una super maggioranza per approvare un blocco, essendo poi il consenso basato su PoA (Proof of Authority) si fonda sulla "reputazione" dei validatori piuttosto che non sulla potenza di calcolo.
è comunque sicuramente necessario un monitoraggio continuo della rete e sistemi di identificazione precoce di possibili anomalie o comportamenti sospetti.
Si può inoltre affermare che se nella storia delle criptovalute più famose sono documentati attacchi come il 51% attack, un attacco a EBSI non colpirebbe direttamente i cittadini europei (niente furto di dati) e ne andrebbe a generare una rendita economica per l'attaccante, avendo dunque come unico effetto un impatto reputazionale nell'infrastruttura tecnologica degli stati membri.

Contromisure per attacchi alla persona:

Per ridurre i rischi legati agli attacchi alla persona è necessario un approccio diversificato di soluzioni tecnologiche avanzate unite a formazione degli utenti.
Dal punto di vista tecnico, i wallet EUDI devono integrare sistemi di protezione robusti come l’autenticazione multifattore oltre che la cifratura end to end delle credenziali.
Fondamentale è anche l’impiego di tecniche crittografiche come le zero knowledge proofs, che permettono all’utente di dimostrare un attributo senza condividere informazioni specifiche (ad esempio potrei dimostrare di essere maggiorenne ma senza condividere la mia età).
Sul piano operativo è necessario garantire procedure di revoca e riemissione delle proprie credenziali in caso di compromissione legata a furto d’identità.

La contromisura più potente rimane comunque la prevenzione attraverso campagne informative, interfacce e strumenti, che rendano chiare le implicazioni di ogni condivisione dati.
Solo la combinazione di sicurezza tecnica e responsabilizzazione individuale può proteggere pienamente l'identità digitale rafforzando la fiducia in questi strumenti e riducendo i rischi legati al social engineering.

Contromisure per attacchi da governi o aziende:

Per mitigare il rischio di abusi da parte di attori istituzionali o aziendali è fondamentale che l'infrastruttura EBSI sia progettata e governata secondo principi di trasparenza, accountability (responsabilità dimostrabile, ogni entità che partecipa a EBSI, deve poter essere identificata e rispondere delle proprie azioni tramite meccanismi di tracciabilità) e privacy by design (principio per cui la tutela della privacy deve essere integrata fin dalla progettazione del sistema e non implementata dopo).
In primo luogo il modello public e permissioned limita già l'accesso della rete a soggetti accreditati e riconosciuti nell'ambito dell'European Blockchain Partnership, riducendo così il pericolo di infiltrazioni o utilizzi opachi.
Tuttavia questo non è sufficiente: è necessario che il funzionamento dei nodi e delle transazioni sia soggetto a meccanismi di auditing indipendente (significa che soggetti terzi devono poter controllare periodicamente che non ci siano manipolazioni dei nodi) e a report pubblico (cioè i risultati dell'auditing devono essere resi accessibili ai cittadini), affinché eventuali comportamenti anomali possano essere rilevati e corretti tempestivamente.
Dal lato utente, l'adozione di tecniche come le zero knowledge proofs rappresentano un argine concreto al rischio di sorveglianza eccessiva o profilazione indebita.
A livello normativo, il regolamento eIDAS 2.0 stabilisce limiti stringenti all'uso dell'identità digitale imponendo che l'accesso ai dati sia proporzionato alla finalità dichiarata e soggetto a controlli sovranazionali.
Infine, la presenza di organismi indipendenti di vigilanza e la possibilità di ricorso da parte dei cittadini in caso di abusi sono strumenti essenziali per preservare la fiducia nel sistema.
La protezione degli attacchi di governi o aziende passa comunque, soprattutto da una governance democratica ed europea, capace di esercitare sicurezza e tutela dei diritti fondamentali.

Contromisure per dipendenza da infrastrutture extraeuropee:

Ridurre la dipendenza da infrastrutture e tecnologie extraeuropee rappresenta una priorità strategica per garantire la sovranità digitale europea e rafforzare la resilienza delle infrastrutture come EUDI ed EBSI.
In questa direzione il primo strumento è di natura normativa, infatti, il regolamento eIDAS 2.0 prevede che il portafoglio europeo di identità digitale sia sviluppato e gestito interamente nel perimetro giuridico dell'Unione, rispettando quindi gli standard di sicurezza comunitari e conforme al GDPR.
Il secondo strumento per ridurre la dipendenza dalle tecnologie extraeuropee è rappresentato dallo sviluppo di cloud e infrastrutture in Europa proprio come il progetto Gaia X.

Gaia X ha l'obiettivo di creare un sistema cloud federato, ruotando attorno ai principi di interoperabilità, sicurezza certificata e trasparenza, ogni servizio conforme riceve un Gaia X label.
Infine la cooperazione tra Stati membri attraverso la European Blockchain Partnership e programmi di finanziamento come Digital Europe stanno consentendo di far crescere un ecosistema digitale europeo competitivo nel tentativo di ridurre progressivamente le influenze geopolitiche esterne.
In questo quadro, le contromisure non possono esaurirsi nella sola crescita tecnica ma si fondano su una strategia congiunta che unisce diritto, tecnologia e governance sovranazionale per garantire che l'identità digitale europea rimanga realmente autonoma e conforme ai valori dell'Unione.

CAPITOLO 5: Incongruenze con GDPR

Introduzione a GDPR:

Il Regolamento Generale sulla Protezione dei Dati (General Data Protection Regulation, GDPR) costituisce il quadro normativo di riferimento per la tutela dei dati personali nell'Unione Europea.
Entrato in vigore nel 2018, il GDPR ha introdotto un sistema di regole valide in tutti gli Stati membri, con l'obiettivo di garantire un elevato livello di protezione dei diritti e delle libertà di ogni cittadino, in particolare del diritto alla riservatezza e alla protezione dei dati personali.
Tra i principi cardine vi sono la liceità, correttezza e trasparenza del trattamento, la limitazione delle finalità, la minimizzazione dei dati, l'esattezza dei dati, la limitazione della conservazione, l'integrità e la riservatezza oltre che la responsabilizzazione dei titolari del trattamento.
Il GDPR offre ai cittadini europei una serie di diritti rafforzati come il diritto di accesso, rettifica e cancellazione, portabilità dei dati e opposizione al trattamento, i quali rafforzano il controllo individuale sulle informazioni personali.
Allo stesso tempo introduce obblighi stringenti per titolari e responsabili del trattamento come l'adozione di misure tecniche adeguate, la valutazione d'impatto sulla protezione dei dati (DPIA) e la nomina del Data Protection Officer (DPO).
Di seguito i pilastri e i diritti del GDPR

Pilastri del GDPR:

1. **Liceità, correttezza e trasparenza**

«I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato» (art. 5, par. 1, lett. a).

2. **Limitazione della finalità**

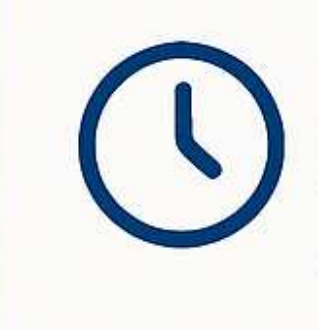
«Raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità» (art. 5, par. 1, lett. b).

3. **Minimizzazione dei dati**

«Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (art. 5, par. 1, lett. c).

4. **Esattezza**

«Esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli affinché i dati inesatti siano cancellati o rettificati tempestivamente» (art. 5, par. 1, lett. d).



5. **Limitazione della conservazione**

«Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità del trattamento» (art. 5, par. 1, lett. e).

6. **Integrità e riservatezza (sicurezza)**

«Trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione […] da trattamenti non

autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, mediante misure tecniche o organizzative adeguate» (art. 5, par. 1, lett. f).

7. **Responsabilizzazione (accountability)**

«Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo» (art. 5, par. 2).

Diritti garantiti dal GDPR:

1. **Diritto all'informazione (Art. 12, 13 e 14)**

Il titolare deve fornire all'interessato informazioni chiare, trasparenti e facilmente accessibili sul trattamento dei dati.
In pratica: privacy policy, informative al momento della raccolta, linguaggio semplice.

2. **Diritto di accesso (Art. 15)**

«L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano […] nonché di accedere ai dati personali e alle informazioni».
In pratica: si può chiedere copia dei dati che l'azienda ha sull'utente.

3. **Diritto di rettifica (Art. 16)**

«L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo».
In pratica: si può chiedere la correzione di dati errati.

4. **Diritto alla cancellazione ("diritto all'oblio") (Art.17)**

«L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo» se ricorrono determinati motivi.
In pratica: si può chiedere che i dati siano eliminati se non più necessari o trattati illecitamente.

5. **Diritto di limitazione del trattamento (Art. 18)**
«L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento» in casi specifici (contestazione esattezza dati, trattamento illecito, ecc.).
In pratica: i dati non vengono cancellati, ma "congelati".

6. **Diritto alla portabilità dei dati (Art. 20)**
«L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano […] e ha il diritto di trasmettere tali dati a un altro titolare».
In pratica: si possono scaricare i propri dati e trasferirli (es. da un social a un altro).

7. **Diritto di opposizione (Art. 21)**
«L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali […] compresa la profilazione».
In pratica: si può dire "no" a determinati trattamenti (marketing, profilazione).

8. **Diritti relativi alle decisioni automatizzate, compresa la profilazione (Art. 22)**
«L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato […] che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

In pratica: no a decisioni solo di algoritmi (es. rifiuto automatico di un prestito) senza intervento umano.

Incompatibilità:

La letteratura scientifica recente ha messo in luce diverse tensioni strutturali tra le caratteristiche tecniche delle blockchain pubbliche e le normative del regolamento generale sulla protezione dei dati.
Nell'articolo di Rahime Belen-Saglam , Enes Altuncu , Yang Lu, Shujun Li viene fatta una revisione sistematica della letteratura (SLR, Systematic Literature Review) che analizza 114 fonti, vengono dunque identificate tre aree di incompatibilità.
In primo luogo, la difficoltà di esercitare i diritti degli interessati, in particolare il diritto all'oblio sancito nell'articolo 17 del GDPR, infatti la natura immutabile e distribuita delle blockchain rende di fatto impossibile cancellare e modificare dati una volta registrati, creando un evidente conflitto con l'obbligo di consentirne l'eliminazione se l'utente lo dovesse richiedere.
In secondo luogo, c'è scarsa chiarezza riguardo al ruolo di titolare e responsabile del trattamento, se il GDPR impone l'individuazione di soggetti chiaramente responsabili delle decisioni sul trattamento dei dati, le blockchain permissionless si fondano sulla decentralizzazione, ci sono quindi diversi nodi che partecipano al consenso ma non esiste un'autorità centrale definita.
Infine vengono sottolineate alcune incertezze sull'applicabilità della legge e sulla giurisdizione, essendo registri distribuiti a livello globale è complesso stabilire quale normativa debba prevalere in caso di conflitti o richieste di accesso ai dati da parte di autorità esterne.
Queste incongruenze mostrano come l'integrazione della blockchain nei sistemi di identità digitale europei e in particolare nell'iniziativa EUDI (e quindi anche di EBSI) impone un'attenta riflessione su come sviluppare il principio di immutabilità e trasparenza tipico delle blockchain integrandolo con i diritti fondamentali cioè la protezione dei dati e la cancellazione, previsti dal quadro normativo europeo.
Vediamo adesso nel dettaglio le incompatibilità relative ad alcune delle aree tematiche:

diritto all'oblio e immutabilità della blockchain:
Una delle problematiche più discusse riguarda l'articolo 17 del GDPR, che riconosce agli interessati il diritto alla cancellazione dei propri dati personali, appunto diritto all'oblio.
In una blockchain permissionless, le informazioni, una volta registrate, non possono essere eliminate senza compromettere la coerenza dell'intera catena.

Anche tecniche come la pseudonimizzazione o l'oscuramento dei dati non garantiscono una cancellazione effettiva, perché le informazioni rimangono permanentemente accessibili.
Questo contrasta con l'esigenza normativa di consentire la rimozione o rettifica dei dati a tutela della privacy individuale.
La letteratura propone diverse soluzioni.
In particolare, la prima è la strategia off chain, secondo cui bisognerebbe memorizzare sulla catena solo riferimenti, cioè hash o puntatori che consentono solo di verificarne l'integrità e non i dati personali.
In questa maniera se l'utente decidesse di eliminare i dati, lo farebbe dal sistema esterno senza modificare il registro distribuito.
La seconda proposta include la cifratura dei dati, se l'utente effettuasse una richiesta di cancellazione, basterebbe distruggere la chiave per rendere i dati illeggibili.
Rimane tuttavia irrisolto il problema connesso al diritto di rettifica dei dati (art. 16 GDPR).
La caratteristica di immutabilità, propria delle blockchain si pone in contrasto aperto, oltre che con la cancellazione (RTBF, Right To Be Forgotten), anche con l'esigenza, sancita dal regolamento, di consentire agli interessati la modifica di informazioni inesatte o incomplete.
La letteratura, per mitigare tale incongruenza, suggerisce un approccio alternativo alla sostituzione diretta dei dati, l'inserimento di un nuovo blocco che indichi l'avvenuta rettifica, preservando così la coerenza della catena e garantendo, al contempo, la tracciabilitá delle modifiche.

attribuzione delle responsabilità (Accountability):
La seconda criticità riguarda l'individuazione del titolare del trattamento (il data controller) e del responsabile del trattamento (il data processor).
Il GDPR richiede che vi sia un soggetto unico, responsabile delle finalità e delle modalità del trattamento dei dati.
Nella blockchain pubblica invece, la governance è decentralizzata, ogni nodo partecipa alla convalida delle transazioni e alla gestione del registro quindi tale distribuzione rende difficile stabilire chi sia il responsabile giuridico, in caso di violazioni e memorizzazione.
In un modello in cui tutti possiedono i dati non è possibile assegnare la responsabilità a un solo individuo o ente.
Questa opacità rappresenta chiaramente, un ostacolo rilevante al soddisfacimento del settimo pilastro del GDPR, quello sull'accountability (Art.5, par.2).

CAPITOLO 6: Conclusioni e prospettive future

Tutela della privacy:

La protezione della privacy rappresenta una sfida cruciale nell'implementazione dell'identità digitale europea, e dell'infrastruttura blockchain EBSI.
Il nuovo regolamento eIDAS 2.0 pone grande enfasi sui principi di privacy by design e data minimisation, imponendo che i portafogli digitali europei integrino tecnologie avanzate per la tutela dei dati personali.
In particolare, gli Stati membri dovranno adottare soluzioni crittografiche come le Zero Knowledge Proof, ZKP che consentono di verificare gli attributi o le dichiarazioni senza rivelare ulteriori dati personali.
Questo approccio garantisce un elevato livello di riservatezza ed evita di dover trasferire più informazioni di quelle strettamente necessarie.
Dal punto di vista architetturale e tecnologico, l'infrastruttura EUDI/EBSI adotta accorgimenti per gestire l' immutabilità della blockchain e il diritto alla rettifica e cancellazione dei dati (GDPR).
Nessun dato personale degli utenti viene memorizzato on-chain sulla blockchain, solo identificatori e attestazioni crittografiche, le informazioni sensibili risiedono infatti off-chain nei dispositivi degli utenti.
Questo design, unito all'uso di hash e puntatori permette di eliminare o modificare i dati off-chain senza modificare la blockchain, soddisfacendo così i requisiti del diritto all'oblio e alla rettifica.
Inoltre i dati e le credenziali presenti nel portafoglio, sono conservati localmente in forma cifrata sotto il pieno controllo dell'utente.
Tutto ciò permette quindi anche di ridurre sensibilmente il rischio di profilazione.
Un altro meccanismo chiave è la divulgazione selettiva degli attributi, infatti il wallet permette di condividere con le relying party (l'ente richiedente) solo gli attributi strettamente necessari, rispettando anche così il principio di minimizzazione dei dati.
Inoltre per prevenire possibili abusi, gli issuer delle credenziali (le entità che emettono i dati gli utenti) non vengono informati quando un utente utilizza i loro attestati, impedendo quindi anche i tracciamenti indiretti.
Non sarà possibile nemmeno, la raccolta di dati sulle transazioni effettuate a cui quindi, non avrà accesso nessun tipo di entità.
Dal punto di vista normativo e organizzativo, sono state predisposte misure per garantire che l'implementazione del portafoglio EUDI sia conforme agli standard di sicurezza e privacy europei.

Il codice sorgente dei componenti software del wallet dovrà essere open source (eccetto per piccoli componenti server side), favorendo così la trasparenza e rendere possibili verifiche indipendenti.
L'ENISA, agenzia UE per la cybersicurezza è stata incaricata di definire schemi di certificazione oltre che verifiche periodiche sul wallet.
I nodi dell'infrastruttura EBSI, saranno gestiti da organizzazioni autorizzate e vigilate e dovranno soddisfare rigorosi requisiti tecnici e legali.
Questa sovranità tecnologica europea assicurerà di rimanere sotto la giurisdizione europea ai dati sensibili di ogni suo cittadino, al riparo da accessi non autorizzati di attori extraeuropei.
In sintesi, l'ecosistema EUDI è progettato dal principio per conciliare innovazione e tutela della privacy, combinando obblighi normativi stringenti, con soluzioni tecnico crittografiche avanzate pensate per garantire all'utente il totale controllo sui propri dati personali.

Ampliamento casi applicabilità:

L'EUDI wallet nasce come strumento generale ma già nel 2025 i casi d'uso si stanno estendendo a molteplici settori grazie a sperimentazioni pilota su scala europea.
L'Unione ha finanziato a partire dal 2023 quattro progetti pilota su larga scala coinvolgendo complessivamente oltre 350 enti pubblici e privati, con lo scopo di testare sul campo le specifiche tecniche del portafoglio EUDI e raccogliere feedback prima del lancio ufficiale nei vari paesi.
Ciascun consorzio pilota (sono quattro) è focalizzato su determinati ambiti applicativi, di seguito vengono descritti alcuni settori in cui il wallet sta dimostrando le sue potenzialità:

- Servizi pubblici e mobilità, il portafoglio EUDI può facilitare l'accesso ai servizi per la pubblica amministrazione e la fruizione di documenti digitali di viaggio. Ad esempio, è possibile presentare una credenziale di identità o un passaporto digitale per richiedere online un documento (come il rinnovo della patente ad esempio) oppure per superare più rapidamente i controlli aeroportuali o doganali. L'EUDI Wallet Consortium, sta proprio sperimentando credenziali di viaggio interoperabili in tutti gli Stati membri, così da permettere il riconoscimento immediato di documenti come passaporti, visti, o patenti di guida in formato digitale.
- Finanza e pagamenti, l'identità digitale europea punta a semplificare le transazioni economiche, assicurando elevati standard di sicurezza e conformità antiriciclaggio. Si potrà usare il wallet per aprire un conto bancario online senza fornire fisicamente i propri documenti ma comunque mantenendo un identificazione certificata. Analogamente si potrà utilizzare il wallet nei

pagamenti digitali su eCommerce, accertando la propria identità e quindi autorizzando pagamenti, senza il bisogno di digitare i dati della carta ad ogni pagamento. Di questo si occupa il consorzio NOBID che ha l'obiettivo di testare pagamenti e servizi bancari integrati con il wallet EUDI (tra i paesi costituenti del consorzio vi è anche l'Italia e tra i partner conta anche Poste italiane).

- Sanità e servizi socio sanitari, il portafoglio digitale europeo offre nuove opportunità per gestire in maniera sicura ed efficiente dati sanitari e certificati medici a livello transfrontaliero. Un caso d'uso rilevante in fase di test riguarda le prestazioni elettroniche ePrescription, grazie al wallet, un cittadino può ricevere una attestazione digitale della ricetta dal proprio sistema sanitario nazionale e presentarla in una farmacia anche al di fuori del suo paese di provenienza. Ciò garantisce l'accesso alle cure anche in mobilità per i cittadini europei semplicemente mostrando il proprio EUDI wallet.
- Educazione e qualifiche professionali, anche il settore dell'educazione e del riconoscimento delle competenze beneficia dell'identità digitale, il wallet infatti, supporta la memorizzazione di diplomi, certificati e altri titoli di studio in formato digitale verificabile. Un neolaureato ad esempio potrebbe inserire nel proprio wallet, il certificato di laurea digitale firmato dall'Università e potrebbe, sempre digitalmente, condividerlo con un datore di lavoro o un altro ente di formazione che lo richieda. In questo ambito opera il consorzio DC4EU (Digital Credential for Europe), il quale sta fornendo il supporto pratico per l'implementazione di credenziali digitali nell'istruzione.

Questi esempi illustrano l'ampiezza crescente dei casi d'uso del wallet.
Sono comunque in corso altre sperimentazioni, ad esempio nell'ambito delle telecomunicazioni (registrazione dell'utente per l'attivazione di SIM mobile), le firme elettroniche, ampiamente citate nel testo, ecc.
L'adozione ufficiale è prevista, in maniera progressiva, da inizio 2026 e si prevede che il wallet EUDI diventi un applicazione a utilizzo trasversale capace di semplificare procedure oltre che promuovere la sovranità tecnologica europea.
In conclusione, l'evoluzione dell'ecosistema EUDI ed EBSI mostrerà come è possibile coniugare tutela della privacy e ampia applicabilità, l'utente rimarrà il padrone dei suoi dati mentre nuove applicazioni pratiche fioriranno in diversi ambiti, da quello finanziario a quello sanitario, portando l'Europa verso un futuro digitale più sicuro, interoperabile e user centric

Bibliografia:

- Buterin, V. (2014). Ethereum white paper: A next generation smart contract & decentralized application platform. Ethereum Foundation. https://ethereum.org/en/whitepaper/

- Commissione Europea. (2014). Regolamento (UE) n.910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 relativo all'identificazione elettronica e ai servizi fiduciari per le transazioni elettroniche nel mercato interno (eIDAS). https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32014R0910

- Commissione Europea. (2021). Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

- Commissione Europea. (2023). Regolamento eIDAS 2.0. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

- European Blockchain Partnership (EBP). (2019). European Blockchain Services Infrastructure (EBSI): Vision and Use Cases. https://ec.europa.eu/digital-strategy/our-policies/european-blockchain-services-infrastructure_en

- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

- Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126. https://dl.acm.org/doi/10.1145/359340.359342

- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson. https://www.pearson.com/en-us/subject-catalog/p/cryptography-and-network-security-principles-and-practice/P200000002788

- W3C. (2019). Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations. World Wide Web Consortium. https://www.w3.org/TR/did-core/

- W3C. (2022). Verifiable Credentials Data Model v1.1. World Wide Web Consortium. https://www.w3.org/TR/vc-data-model/

- Parlamento Europeo. (2023). Indagine sull'uso di Pegasus e di spyware di sorveglianza equivalenti. https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA(2023)747923_IT.pdf

- Rahime Belen-Saglam, Enes Altuncu, Yang Lu, and Shujun Li. A systematic literature review of the tension between the gdpr and public blockchain systems. Blockchain: Research and Applications, 4(2): 100129, 2023, https://www.sciencedirect.com/science/article/pii/S2096720923000040

- European Commission. (2023). Architecture and Reference Framework (ARF) for the European Digital Identity Wallet, v1.1.0. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/arf/

- Commissione Europea. (2023). EU Digital Identity Wallet: Four large-scale pilot projects. https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-wallet-four-large-scale-pilot-projects

- ENISA. (2023). Supporting the EU Digital Identity Wallet ecosystem. https://www.enisa.europa.eu/news/enisa-news/supporting-the-eu-digital-identity-wallet-ecosystem

- European Commission. (2025). European Digital Identity Wallet – Common Toolbox and pilot use cases. https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet

- NOBID Consortium. (2023). EUDI Wallet Large Scale Pilot for Payments. https://nobidconsortium.com

- POTENTIAL Consortium. (2023). Piloting the European Digital Identity Wallet.
  https://potential-project.eu

- DC4EU Consortium. (2023). Digital Credentials for Europe (DC4EU).
  https://dc4eu.eu